

FILED

UNITED STATES DISTRICT COURT

MAY 29 2025

for the

Northern District of Oklahoma

Heidi D. Campbell, Clerk
U.S. DISTRICT COURT

In the Matter of the Search of)
 Information Associated with Facebook User IDs)
 "61556739013627," "jeremy.sertich.1,")
 "61560988455037," and "61556408047701" that are)
 Stored at a Premises Controlled by Meta Platforms, Inc.)

Case No. 25-mj-458-mts**FILED UNDER SEAL****APPLICATION FOR A SEARCH WARRANT**

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (*identify the person or describe the property to be searched and give its location*):

See Attachment "A." This court has authority to issue this warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A).
 located in the Northern District of California, there is now concealed (*identify the person or describe the property to be seized*):

See Attachment "B"

The basis for the search under Fed. R. Crim. P. 41(c) is (*check one or more*):

- ☒ evidence of a crime;
☒ contraband, fruits of crime, or other items illegally possessed;
☒ property designed for use, intended for use, or used in committing a crime;
☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

*Code Section**Offense Description*

18 U.S.C. § 2423(a)

Transportation of a Minor with Intent to Engage in Criminal Sexual Activity

18 U.S.C. § 2422(b)

Coercion or Enticement of a Minor to Engage in Sexually Explicit Activity

18 U.S.C. §§ 2252(a)(2) and (b)(1)

Receipt of Child Pornography

18 U.S.C. §§ 2252(a)(4)(B) and (b)(2)

Possession of and Access with Intent to View Child Pornography

The application is based on these facts:

See Affidavit of TFO Austin C. Duncan, attached hereto.

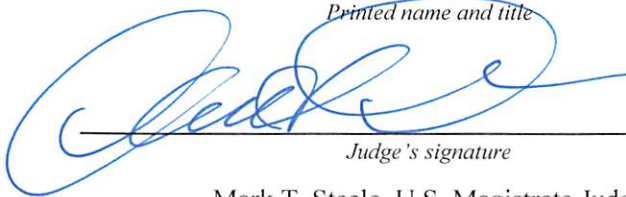
- ☒ Continued on the attached sheet.
☐ Delayed notice of ____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

*Applicant's signature*

TFO Austin C. Duncan

Printed name and title

Subscribed and sworn to by phone.

Date: 5-29-2025*Judge's signature*City and state: Tulsa, Oklahoma

Mark T. Steele, U.S. Magistrate Judge

Printed name and title

**IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF OKLAHOMA**

**In the Matter of the Search of
Information Associated with Facebook
User IDs “61556739013627,”
“jeremy.sertich.1,”
“61560988455037,” and
“61556408047701” that are Stored at a
Premises Controlled by Meta
Platforms, Inc.**

Case No. _____

FILED UNDER SEAL

Affidavit in Support of an Application for a Search Warrant

I, Austin C. Duncan, being first duly sworn under oath, depose and state:

Introduction and Agent Background

1. I make this affidavit in support of an application for a search warrant for information associated with the Facebook account user IDs “61556739013627,” “jeremy.sertich.1,” “61560988455037,” and “61556408047701” that are stored at a premises owned, maintained, controlled, or operated by Meta Platforms, Inc. (“Meta”), an electronic communications service and/or remote computing service provider headquartered at 1601 Willow Road in Menlo Park, California. The information to be searched is described in the following paragraphs and in Attachment A. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require Meta to disclose to the government information (including the content of communications) in its possession, pertaining to the subscribers or customers associated with the user

IDs “61556739013627,” “jeremy.sertich.1,” “61560988455037,” and “61556408047701” as further described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review the information to locate the items described in Section II of Attachment B.

2. I am a federal law enforcement officer as defined under Rule 41(a)(2)(C) and am authorized to request this search warrant because I am a government agent who is engaged in enforcing federal criminal laws and I am within the category of officers authorized by the Attorney General to request such a warrant.

3. I have been employed with the Oklahoma Highway Patrol (OHP) since January 2015. I am an Investigator assigned to Troop Z, Criminal Investigations Division and assigned as a Task Force Officer with Homeland Security Investigations (HSI) Tulsa. During my tenure as a criminal investigator, I participated as a case agent and support agent in numerous investigations, covering various areas of criminal law. During these investigations, I participated in interviewing witnesses, suspects, and sources regarding these various crimes, and I read official reports of similar interviews by other investigators. I have participated in surveillance operations, observing and recording movements of persons involved in criminal activity. I have authored search warrants in furtherance of criminal investigations. I have also spoken on numerous occasions with other experienced investigators concerning the methods and practices of criminal enterprises and drug

traffickers. I completed and became certified as “Customs Officer” after attending HSI’s Title 19 training course. The training specialized in authorities granted as a Customs Officer in Title 19, United States Code (USC), Section 1401(i); 19 U.S.C 1589a. The training covered criminal laws and investigative authorities granted under these provisions. Through my training and experience, I am familiar with the methods used by criminal organizations to smuggle, safeguard, and to collect and launder illicit proceeds. I am further aware of the methods employed by criminal organizations to advance their criminal enterprise and thwart any investigation into their activities. As a result of my employment with HSI, my duties include, but are not limited to, the investigation and enforcement of Titles 18 and 19 of the United States Code (U.S.C.). Moreover, I am a federal law enforcement officer who is engaged in enforcing the criminal laws, including 18 U.S.C. §§ 2251, 2252, 2422, and 1343.

4. I am familiar with the facts and circumstances of this investigation. The facts set forth in this affidavit are based on my personal observations, knowledge obtained from other law enforcement officers, my review of documents related to this investigation, conversations with others who have personal knowledge of the events and circumstances described herein, and a review of open-source information including information available on the Internet. Because this affidavit is submitted for the limited purpose of establishing probable cause in support of the application

for a search warrant, it does not set forth each and every fact I or others have learned during the course of this investigation.

5. Based on my training, experience, and the facts as set forth in this affidavit, there is probable cause to believe the identified Facebook account contains evidence, instrumentalities, contraband, and/or fruits of violations of Title 18 United States Code § 2423(a) (Transportation of a Minor with Intent to Engage in Criminal Sexual Activity); 18 U.S.C. § 2422(b), (Coercion or Enticement of a Minor to Engage in Sexually Explicit Activity); 18 U.S.C. §§ 2252(a)(2) and (b)(1) (Receipt of Child Pornography); and 18 U.S.C. §§ 2252(a)(4)(B) and (b)(2) (Possession of and Access with Intent to View Child Pornography), exists and will be located in the electronically stored information described in Attachment B and is recorded on the device described in Attachment A.

Jurisdiction

6. This Court has jurisdiction to issue the requested warrant because it is “a court of competent jurisdiction” as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A), & (c)(1)(A). Specifically, the Court is “a district court of the United States . . . that has jurisdiction over the offense being investigated.” 18 U.S.C. § 2711(3)(A)(i).

7. When the government obtains records pursuant to § 2703, or pursuant to a search warrant, the government is not required to notify the subscriber of the existence of the warrant. 18 U.S.C. § 2703(a), (b)(1)(A), (c)(2), and (3). Additionally,

the government may obtain an order precluding Meta from notifying the subscriber or any other person of the warrant, for such period as the Court deems appropriate, where there is reason to believe that such notification will seriously jeopardize the investigation. 18 U.S.C. § 2705(b).

Characteristics Common to Individuals Who Exhibit a Sexual Interest in Children

8. Based on my previous investigative experience related to child exploitation investigations, and the training and experience of other law enforcement officers with whom I have had discussions, I know there are certain characteristics common to individuals who exhibit a sexual interest in children:

- a. Such individuals may receive sexual gratification, stimulation, and satisfaction from contact with children, or from fantasies they may have viewing children engaged in sexual activity or in sexually suggestive poses, such as in person, in photographs, or other visual media, or from literature describing such activity;
- b. Such individuals may collect sexually explicit or suggestive materials in a variety of media, including photographs, magazines, motion pictures, videotapes, books, slides and/or drawings or other visual media. Individuals who have a sexual interest in children or images of children oftentimes use these materials for their own sexual arousal and gratification. Further, they may use these materials

to lower the inhibitions of children they are attempting to seduce, to arouse the selected child partner, or to demonstrate the desired sexual acts;

c. Such individuals typically possess and maintain digital or electronic files of child pornographic material, that is, their pictures, videos, photographs, correspondence, mailing lists, etc., in a secure location. Individuals who have a sexual interest in children or images of children typically retain pictures, videos, photographs, correspondence, and mailing lists for many years;

d. Likewise, such individuals often maintain their child pornography images in a digital or electronic format in a safe, secure and private environment, such as a computer and surrounding area. These child pornography images are often maintained for several years and are kept close by, usually at the possessor's residence, inside the possessor's vehicle, or, at times, on their person, to enable the individual to view the child pornography images, which are valued highly. Some of these individuals also have been found to download, view, and then delete child pornography on their computers or digital devices on a cyclical and repetitive basis;

e. Based on my training and experience and speaking with other special agents, I know that such individuals have taken their electronic devices and storage media, which contain their collections of child pornography, with them when they have moved or changed residences;

f. Such individuals may also take it upon themselves to create their own child pornography or child erotica images, videos or other recordings. These images, videos or other recordings may be taken or recorded covertly, such as with a hidden camera in a bathroom, or the individual may have child victims he or she is abusing in order to produce child pornographic or child erotica images, videos or other recordings. These images, videos or other recordings are often collected, traded, or shared;

g. Importantly, evidence of such activity, including deleted child pornography, often can be located on these individuals' computers and digital devices through the use of forensic tools. Indeed, the very nature of electronic storage means that evidence of the crime is often still discoverable for extended periods of time even after the individual "deleted"¹ it;

h. Such individuals also may correspond with and/or meet others to share information and materials, rarely destroy correspondence from other child pornography distributors/possessors, conceal such correspondence as they do their sexually explicit material, and often maintain lists of names, addresses, and

¹ See *United States v. Carroll*, 750 F.3d 700, 706 (7th Cir. 2014) (concluding that 5-year delay was not too long because "staleness inquiry must be grounded in an understanding of both the behavior of child pornography collectors and of modern technology"); see also *United States v. Seiver*, 692 F.3d 774 (7th Cir. 2012) (Posner, J.) (collecting cases, e.g., *United States v. Allen*, 625 F.3d 830, 843 (5th Cir. 2010); *United States v. Richardson*, 607 F.3d 357, 370–71 (4th Cir. 2010); *United States v. Lewis*, 605 F.3d 395, 402 (6th Cir. 2010).)

telephone numbers of individuals with whom they have been in contact and who share the same interests in child pornography;

i. Such individuals may use social media applications or other means of electronic communications to locate, converse with, and groom minor victims in an attempt to solicit child pornography and/or physically meet and sexually abuse a minor victim;

j. Such individuals who use social media applications or other means of electronic communications to locate, converse with, and groom minor victims often do not just have one victim. It has been my experience in these types of investigations that such individuals will communicate with multiple victims in an attempt to be more successful in obtaining child pornography and/or physically meeting and abusing a victim;

k. Based on my training and experience, I know that such individuals may use their financial information to buy and sell child pornography online and purchase software used to mask their online activity from law enforcement. For instance, individuals may purchase cryptocurrency such as Bitcoin to buy and sell child pornography online. The use of cryptocurrency provides a level of anonymity because it masks the user's identity when conducting online financial transactions and provides a means of laundering illicit proceeds. Financial information may provide a window into the identities of individuals seeking to buy or sell child pornography online by tying the illicit transactions back to the user. Financial

information contained on an electronic device containing child pornography may also provide indicia of ownership. Further, based on my training and experience, I know that individuals involved in the trafficking of child pornography may use sophisticated software, such as router configuration software, virtual private networks, proxy servers, cryptocurrency exchanges, or other anonymizing software, in conjunction with these illicit financial transactions to provide dual layers of anonymity and prevent law enforcement detection. Financial information may indicate which services were purchased to obscure an individual's identity;

9. Such individuals prefer not to be without their child pornography for any prolonged period of time. This behavior has been documented by law enforcement officers involved in the investigation of child pornography throughout the world.

Meta Background

10. Meta owns and operates Facebook, a free-access social networking website of the same name that can be accessed at <http://www.facebook.com>. Facebook users can use their accounts to share communications, news, photographs, videos, and other information with other Facebook users, and sometimes with the general public.

11. Meta asks Facebook users to provide basic contact and personal identifying information to Facebook, either during the registration process or thereafter. This information may include the user's full name, birth date, gender, e-mail addresses,

physical address (including city, state, and zip code), telephone numbers, screen names, websites, and other personal identifiers. Each Facebook user is assigned a user identification number and can choose a username.

12. Facebook users may join one or more groups or networks to connect and interact with other users who are members of the same group or network. Facebook assigns a group identification number to each group. A Facebook user can also connect directly with individual Facebook users by sending each user a “Friend Request.” If the recipient of a “Friend Request” accepts the request, then the two users will become “Friends” for purposes of Facebook and can exchange communications or view information about each other. Each Facebook user’s account includes a list of that user’s “Friends” and a “News Feed,” which highlights information about the user’s “Friends,” such as profile changes, upcoming events, and birthdays.

13. Facebook users can select different levels of privacy for the communications and information associated with their Facebook accounts. By adjusting these privacy settings, a Facebook user can make information available only to himself or herself, to particular Facebook users, or to anyone with access to the Internet, including people who are not Facebook users. A Facebook user can also create “lists” of Facebook friends to facilitate the application of these privacy settings. Facebook accounts also include other account settings that users can adjust to control, for example, the types of notifications they receive from Facebook.

14. Facebook users can create profiles that include photographs, lists of personal interests, and other information. Facebook users can also post “status” updates about their whereabouts and actions, as well as links to videos, photographs, articles, and other items available elsewhere on the Internet. Facebook users can also post information about upcoming “events,” such as social occasions, by listing the event’s time, location, host, and guest list. In addition, Facebook users can “check in” to particular locations or add their geographic locations to their Facebook posts, thereby revealing their geographic locations at particular dates and times. A particular user’s profile page also includes a “Wall,” which is a space where the user and his or her “Friends” can post messages, attachments, and links that will typically be visible to anyone who can view the user’s profile.

15. Facebook users can upload photos and videos to be posted on their Wall, included in chats, or for other purposes. Users can “tag” other Facebook users in a photo or video and can be tagged by others. When a user is tagged in a photo or video, he or she generally receives a notification of the tag and a link to see the photo or video.

16. Facebook users can use Facebook Messenger to communicate with other users via text, voice, and video. Meta retains instant messages and certain other shared Messenger content unless deleted by the user, and also retains transactional records related to voice and video chats, including the date of each call. Facebook users can also post comments on the Facebook profiles of other users or on their own

profiles; such comments are typically associated with a specific posting or item on the profile.

17. If a Facebook user does not want to interact with another user on Facebook, the first user can “block” the second user from seeing his or her account.

18. Facebook has a “like” feature that allows users to give positive feedback or connect to particular pages. Facebook users can “like” Facebook posts or updates, as well as webpages or content on third-party (*i.e.*, non-Facebook) websites. Facebook users can also become “fans” of particular Facebook pages.

19. Facebook has a search function that enables its users to search Facebook for keywords, usernames, or pages, among other things.

20. Each Facebook account has an activity log, which is a list of the user’s posts and other Facebook activities from the inception of the account to the present. The activity log includes stories and photos that the user has been tagged in, as well as connections made through the account, such as “liking” a Facebook page or adding someone as a friend. The activity log is visible to the user but cannot be viewed by people who visit the user’s Facebook page.

21. Facebook also has a Marketplace feature, which allows users to post free classified ads. Users can post items for sale, housing, jobs, and other items on the Marketplace.

22. In addition to the applications described above, Meta provides users with access thousands of other applications (“apps”) on the Facebook platform. When a

Facebook user accesses or uses one of these applications, an update about that the user's access or use of that application may appear on the user's profile page.

23. Meta also retains records of which IP addresses were used by an account to log into or out of Facebook, as well as IP address used to take certain actions on the platform. For example, when a user uploads a photo, the user's IP address is retained by Meta along with a timestamp.

24. Meta retains location information associated with Facebook users under some circumstances, such as if a user enables "Location History," "checks-in" to an event, or tags a post with a location.

25. Social networking providers like Meta typically retain additional information about their users' accounts, such as information about the length of service (including start date), the types of service utilized, and the means and source of any payments associated with the service (including any credit card or bank account number). In some cases, Facebook users may communicate directly with Meta about issues relating to their accounts, such as technical problems, billing inquiries, or complaints from other users. Meta typically retains records about such communications, including records of contacts between the user and the provider's support services, as well as records of any actions taken by the provider or user as a result of the communications.

26. As explained herein, information stored in connection with a Facebook account may provide crucial evidence of the “who, what, why, when, where, and how” of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or, alternatively, to exclude the innocent from further suspicion. In my training and experience, a Facebook user’s IP log, stored electronic communications, and other data retained by Meta, can indicate who has used or controlled the Facebook account. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence. For example, profile contact information, private messaging logs, status updates, and tagged photos (and the data associated with the foregoing, such as date and time) may be evidence of who used or controlled the Facebook account at a relevant time. Further, Facebook account activity can show how and when the account was accessed or used. For example, as described herein, Meta logs the Internet Protocol (IP) addresses from which users access their accounts along with the time and date. By determining the physical location associated with the logged IP addresses, investigators can understand the chronological and geographic context of the account access and use relating to the crime under investigation. Such information allows investigators to understand the geographic and chronological context of Facebook access, use, and events relating to the crime under investigation. Additionally, location information retained by Meta may tend to either inculcate or exculpate the Facebook account owner. Last, Facebook account activity may

provide relevant insight into the Facebook account owner's state of mind as it relates to the offense under investigation. For example, information on the Facebook account may indicate the owner's motive and intent to commit a crime (e.g., information indicating a plan to commit a crime), or consciousness of guilt (e.g., deleting account information in an effort to conceal evidence from law enforcement).

27. Therefore, Meta's servers are likely to contain all the material described above, including stored electronic communications and information concerning subscribers and their use of Facebook, such as account access information, transaction information, and other account information.

28. On May 6, 2025, I requested that Meta preserve any information for the accounts listed in Attachment A.

Probable Cause

1. On May 5, 2025, Homeland Security Investigations (HSI) Tulsa received information from the Oklahoma Highway Patrol (OHP) regarding a missing, 16-year-old, minor female from Quapaw, Oklahoma. Later that day, on May 5, 2025, the Minor Victim (MV) was recovered in Duluth, Minnesota with a 33-year-old male subject, later identified as Jeremy SERTICH ("SERTICH").

2. On May 7, 2025, Task Force Officer (TFO) Austin Duncan HSI received a Duluth Police Report stating that on May 2, 2025, Duluth Police Department (DPD) received information from the OHP Child Abduction Response Team

(CART) about a 16 year old female, missing juvenile, MV. The report notes that OHP advised DPD that the MV was believed to be with a person named Jeremy Jon SERTICH, whose date of birth was is **/**/1991 (33 years old). Officer NICHOLAS LEPAK with DPD conducted a records check and discovered SERTICH had history of being employed at the Econolodge in Hermantown, Minnesota. Trooper AARON KERN of OHP CART submitted an exigent request to U.S. Cellular and discovered the MV's phone number and obtained historical pings based on exigent circumstances. Historical pings placed the MV within a half mile of the Econolodge in Hermantown, Minnesota. Trooper AARON KERN of OHP CART submitted an exigent request to U.S. Cellular and discovered the MV's phone number and obtained historical pings based on exigent circumstances. Historical pings placed the MV within a half mile of the Econolodge in Hermantown, Minnesota. Hermantown Police Department (HPD) checked the Econolodge and there was no one by either name staying there. SERTICH had apparently ceased employ at the Econolodge in January of 2025.

3. On May 5, 2025, Captain HOLLI MCDANIEL with the Ottawa County Sheriff's Office created a Missing Person's bulletin, which contained information and photographs of both SERTICH and MV. MCDANIEL distributed the flyer to law enforcement agencies in Oklahoma and two news media outlets in Duluth, Minnesota.

4. OHP CART members stated they had Flock camera images of three vehicles with Minnesota license plates in the vicinity of where MV lived in

Oklahoma, with one belonging to a rental car company, EAN Holdings. OHP CART members were able to identify SERTICH as the person who rented that car by contacting EAN Holdings. OHP CART and Investigators from the Ottawa County Sheriff's Office (OCSO) discovered that SERTICH picked up MV on Friday, May 1, 2025 sometime between 11:00 P.M. and 11:30 P.M., from the area of her residence near Quapaw, Oklahoma. Additional Flock images were obtained of the vehicle where it was observed driving north from Oklahoma, with the last Flock image of the vehicle was observed in Clay County, Missouri in the early morning hours of May 2, 2025.

5. On May 5, 2025, at approximately 5:23 P.M., St. Louis County, Minnesota Dispatch received a call from a staff member at Union Gospel Mission, located at 219 East 1st Street in Duluth, Minnesota, who stated that they had seen the missing persons flyer with MV on the news and stated that the MV had been seen with SERTICH at the apartment complex. After receiving the notification from dispatch, Officer Cole Barkos with DPD contacted the Union Gospel Mission staff member, who stated that SERTICH was renting Unit 212. DPD officers responded to the Union Gospel Mission. Upon arrival, officers positioned themselves outside of apartment #212 and listened outside of the apartment door. The officers heard a male and female voice coming from inside the apartment, which sounded like talking and giggling. Officer Michael Munger knocked on the door and the voices went silent. It took several moments for anyone to answer. A

person, who was later identified as SERTICH, answered the door. Officer Munger asked if the MV was inside the apartment and SERTICH did not say anything. SERTICH leaned back against the wall and sat down on the floor.

6. Munger asked SERTICH if he could have permission to search the apartment for the missing and endangered juvenile. Upon asking SERTICH, he immediately leaned his upper body against the wall and slumped to the floor into a seated position. Due to the high risk and dangerous situation of a missing juvenile, taken across state lines without permission from parents or guardians, Officer Munger and Officer Barkos entered the apartment to ensure the juvenile was safe and in no immediate danger and did not require emergency aid.

7. . Officers entered the apartment, which was a one-bedroom apartment. There was no one seen inside the apartment but there was a closed closet. Officer Munger opened the closet door, and the MV was standing inside naked with a blanket wrapped around her. SERTICH was transported to the DPD Public Safety building for further questioning.

8. The MV was transported to the hospital for a Sexual Assault Nurse Examination (SANE). The MV told officers she met SERTICH on Facebook when she was 13 or 14 years old. MV stated she had been in a sexual relationship with SERTICH for about a year. She told officers, SERTICH picked her up from Oklahoma a couple of days ago, and she was not sure when. MV stated they have been having consensual sex since she had been in Duluth.

9. The MV disclosed to Officers she had sent SERTICH nude pictures of herself and he had sent her nude pictures of himself. The MV had seen SERTICH's phone since she had been in Duluth and saw the nude pictures she sent him still on his phone. MV also disclosed that the day before the interview, Sertich saw the missing person flyer on Facebook, and he became upset about it. The missing person flyer named him and had both of their pictures on it. The MV consented to a SANE which was performed by approved medical staff.

10. In a Mirandized interview with DPD Investigator Ryan Puhle, SERTICH stated MV was his "fiancé", and he had known her since October of 2023 after becoming friends on Facebook. Since that date, SERTICH has met MV in person seven times, including this most recent incident. SERTICH admitted that on April 30, 2025, he rented a car in Duluth, Minnesota and drove to the area of Quapaw, Oklahoma where MV lived at her request and picked her up. SERTICH and MV drove back to Duluth and had been staying there since May 2, 2025. SERTICH admitted to having sexual intercourse with MV on May 4, 2025 at a hotel in Superior, Wisconsin because his apartment did not allow visitors. SERTICH admitted to having sex with MV at his apartment in the Union Gospel Mission. SERTICH said he did not use a condom. SERTICH said that on May 4, 2025, he saw the missing person's bulletin for MV on Facebook and was aware that MV's mother wanted her returned home. SERTICH also admitted to both sending and receiving sexually explicit pictures with MV for months through the use of his

Facebook account and his Google account via email address jjsertich315@gmail.com. SERTICH said he instead rented a car at the airport in Duluth (4701 Grinden Drive) at National Car Rental. He described this as a gray or silver Nissan Sentra or sedan style vehicle. SERTICH did this on April 30, 2025 and drove 13.5 hours to Quapaw, Oklahoma to pick up MV. MV had given him the address on previous occasions, so he knew where to drive and said he used Google maps to guide his route there. He made several stops for gas and food on the way which included a hotel stay so he could sleep and get back on the road to Quapaw.

11. Once SERTICH neared MV's home on May 1, 2025, he agreed to meet MV at "the Y". SERTICH described this as a roadway near her home which splits into a Y fashion. SERTICH said that MV wanted to meet away from her home. SERTICH alleged that he did not care what MV's family would have thought if he had shown up at her home. SERTICH drove with MV to Duluth and had been there since May 2, 2025. SERTICH rented a hotel room in Superior, Wisconsin at the "Quality Inn" (1405 Susquehanna Ave, Superior, WI 54880) because MV asked to take a shower and SERTICH's apartment complex did not allow guests. SERTICH rented this room on May 4, 2025 and admitted to having sex with MV without a condom. He described this act by saying that MV likes to lay on top of his body and whisper into his ear that she is "horny" to initiate sexual intercourse. SERTICH ultimately did sneak MV into his apartment where he again admitted

that he had sexual intercourse with her in Duluth. Sertich said MV was in his apartment watching Gossip Girl on her laptop when he said her bra became uncomfortable, so she removed it. Sertich could specifically recall what she was wearing on her bottom half but believed she had underwear on when DPD knocked at his door. He recalled looking through the peep hole on his door and seeing DPD and verbally telling MV something to the effect of “fuck it’s the cops.” SERTICH denied asking MV to hide in his closet.

12. SERTICH admitted to using his phone to access his Facebook account to speak with MV and to send and receive sexual messages and pictures. SERTICH did not know his Facebook username but said he used the cell phone found in his apartment to do this. This phone was ultimately seized and submitted to DPD evidence storage and placed on a portable charger and into a faraday bag. SERTICH also admitted to using his phone to access his google account to communicate with MV. He stated his email address for this account is jjsertich315@gmail.com and that he would also send and receive sexual messages, pictures, and videos with MV. He said he would send pictures of himself when MV would ask for them and that he would sometimes ask her for naked photographs as well. SERTICH also said MV would randomly send him pictures and videos of her naked body, citing a recent example of MV sending him a video of her in the shower.

13. On May 5, 2025, after the interviews of MV and SERTICH, at approximately 10:55 P.M., DPD officers executed a search warrant at 219 E 1st Steet, Apartment 212, Duluth, Minnesota 55802. Pursuant to the parameters of the search warrant, DPD officers collected a blue Motorola (Android) phone from the apartment. The items were collected and transported to DPD Headquarters and placed into evidence. The Motorola phone was later transported and stored at Douglas County Sheriff's Office, Lake Superior Forensic Technology and Internet Crimes Against Children Forensic Laboratory located at 1316 North 14th Street, Ste 100, Superior, Wisconsin, where it is currently located.

14. On May 6, 2025, Investigator Puhle went to EAN Holdings, LLC car rental at the airport to get information from them. SERTICH rented a car to go to Oklahoma to pick MV up. While at the car rental, EAN Holdings informed Investigator Puhle there was a phone located in the car after the rental. The MV told Officer Munger that she lost her phone and believed she lost it in the car they rented. Investigator Puhle spoke to MV's mother, who stated she was the owner of the phone and gave Investigator Puhle permission to seize the phone. The vehicle that was rented by SERTICH was a 2025 Nissan Sentra Sedan bearing Minnesota plate RRY044, with a vehicle identification number of 3N1AB8CV2SY276101. Minnesota license plate RRY044 matched the license plate of the vehicle observed on Flock images that traveled to the area where MV lived on May 1, 2025, and also was seen driving north from Oklahoma in the early morning hours of May 2, 2025.

15. On May 6, 2025, Investigator Puhle responded to the Quality Inn at 1405 Susquehanna Avenue, Superior, Wisconsin 54880. Investigator Puhle spoke with the attendant at the desk who identified herself as Darlene Jo Renquist. Renquist provided a printout of SERTICH's booking information. This booking showed that SERTICH arrived on May 4, 2025 at 2:50 P.M. and checked out on May 5, 2025 at 12:28 P.M. Sertich paid \$87.75 for the room, and it was charged under a credit card with the last 4 numbers being 7728. SERTICH stayed in room #214, but Renquist said she was told by other staff members that SERTICH stayed in room #215.

Information to be Searched and Things to be Seized

16. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant. The government will execute this warrant by serving it on Meta. Because the warrant will be served on Meta, who will then compile the requested records at a time convenient to it, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night.

17. I anticipate executing this warrant under the Electronic Communications Privacy Act, in particular 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A), by using the warrant to require Meta to disclose to the government digital copies of the records and other information (including the content of communications) particularly described in Section I of Attachment B. Upon receipt of the information

described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

18. In conducting this review, law enforcement personnel may use various methods to locate evidence and instrumentalities of the crime(s) under investigation, including but not limited to undertaking a cursory inspection of all information within the account described in Attachment A. This method is analogous to cursorily inspecting all the files in a file cabinet in an office to determine which paper evidence is subject to seizure. Although law enforcement personnel may use other methods as well, particularly including keyword searches, I know that keyword searches and similar methods are typically inadequate to detect all information subject to seizure. As an initial matter, keyword searches work only for text data, yet many types of files commonly associated with e-mails, including attachments such as scanned documents, pictures, and videos, do not store data as searchable text. Moreover, even as to text data, keyword searches cannot be relied upon to capture all relevant communications in an account as it is impossible to know in advance all of the unique words or phrases investigative subjects will use in their communications, and consequently there are often many communications in an account that are relevant to an investigation but do not contain any searched keywords.

Conclusion

19. Based on the information above, I submit that there is probable cause to believe that there is evidence of violations of 18 U.S.C. § 2423(a) (Transportation of

a Minor with Intent to Engage in Criminal Sexual Activity); 18 U.S.C. § 2422(b), (Coercion or Enticement of a Minor to Engage in Sexually Explicit Activity); 18 U.S.C. §§ 2252(a)(2) and (b)(1) (Receipt of Child Pornography); and 18 U.S.C. §§ 2252(a)(4)(B) and (b)(2) (Possession of and Access with Intent to View Child Pornography), have been violated, and that evidence of these offenses, more fully described in Attachment B, are associated with the Facebook accounts described in Attachment A.


20. I request to be allowed to share this affidavit and the information obtained from this search (to include copies of digital media) with any government agency, to include state and local agencies investigating or aiding in the investigation of this case or related matters, and to disclose those materials as necessary to comply with discovery and disclosure obligations in any prosecutions from this matter.

Respectfully submitted,



Austin C. Duncan
Task Force Officer
Homeland Security Investigations

Subscribed and sworn to by phone on May ²⁹29, 2025.



MARK T. STEELE
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

Property to be Searched

This warrant applies to information associated with the Facebook account user IDs “61556739013627,” “jeremy.sertich.1,” “61560988455037,” and “61556408047701” that are stored at a premises owned, maintained, controlled, or operated by Meta Platforms, Inc., a company headquartered in Menlo Park, California.

ATTACHMENT B
Particular Things to be Seized

I. Information to be disclosed by Meta Platforms, Inc. (“Meta”)

To the extent that the information described in Attachment A is within the possession, custody, or control of Meta, regardless of whether such information is located within or outside of the United States, including any messages, records, files, logs, or information that has been deleted but is still available to Meta, or has been preserved pursuant to a request made under 18 U.S.C. § 2703(f), Meta is required to disclose the following information to the government for each user ID listed in Attachment A:

A. All business records and subscriber information, in any form kept, pertaining to the Account, including:

1. All contact and personal identifying information, including full name, user identification number, birth date, gender, contact e-mail addresses, physical address (including city, state, and zip code), telephone numbers, screen names, websites, and other personal identifiers.
2. All profile information; News Feed information; status updates; videos, photographs, articles, and other items; Notes; Wall postings; friend lists, including the friends' Facebook user identification numbers; groups and networks of which the user is a member, including the groups' Facebook group identification numbers; future and past event postings;

rejected “Friend” requests; comments; gifts; pokes; tags; and information about the user’s access and use of Facebook applications;

3. All records or other information regarding the devices and internet browsers associated with, or used in connection with, that user ID, including the hardware model, operating system version, unique device identifiers, mobile network information, and user agent string;
4. All IP logs, including all records of the IP addresses that logged into the account;
5. The length of service (including start date) and the means and source of any payments associated with the service (including any credit card or bank account number);
6. All privacy settings and other account settings, including privacy settings for individual Facebook posts and activities, and all records showing which Facebook users have been blocked by the account;
7. All past and present lists of friends created by the account;
8. The types of service utilized by the user;
9. All associated logs and metadata;

B. All content, records, and other information relating to communications sent from or received by the Account from January 1, 2022 through May 5, 2025, including but not limited to:

1. The content of all communications sent from or received by the Account, including direct and group messages, and all associated multimedia and metadata, including deleted and draft content, if available;
2. All activity logs for the account and all other documents showing the user's posts and other Facebook activities from January 1, 2022 through May 5, 2025.
3. All photos and videos uploaded by that user ID and all photos and videos uploaded by any user that have that user tagged in them from January 1, 2022, through May 5, 2025, including Exchangeable Image File ("EXIF") data and any other metadata associated with those photos and videos;
4. All other records and contents of communications and messages made or received by the user from January 1, 2022 through May 5, 2025, including all Messenger activity, private messages, chat history, video and voice calling history, and pending "Friend" requests;
5. All "check ins" and other location information;
6. All records pertaining to communications between Meta and any person regarding the user or the user's Facebook account, including contacts with support services and records of actions taken;

C. All content, records, and other information relating to all other interactions between the Account and other Facebook users from January 1, 2022 through May 5, 2025, including but not limited to:

1. All records of the account's usage of the "Like" feature, including all Facebook posts and all non-Facebook webpages and content that the user has "liked";
2. All information about the user's access and use of Facebook Marketplace;
3. All information about the Facebook pages that the account is or was a "fan" of;

D. All records of Facebook searches performed by the account from January 1, 2022 through May 5, 2025;

E. All location information, including location history, login activity, information geotags, and related metadata from January 1, 2022 through May 5, 2025.

Meta is further ordered to disclose the above information to the government within **14 days** after service of this warrant.

II. Information to be searched for and seized by the government

All information described above in Section I that constitutes evidence, instrumentalities, contraband, and/or fruits of violations of 18 U.S.C. §§ 2251, 2252, 2422, and 1343 for each account or identifier listed on Attachment A:

- a. Information, correspondence, records, documents, or other materials pertaining to the enticement or coercion of minors to engage in sexual acts or sexual conduct, as defined in 18 U.S.C. § 2422(b);
- b. Images of child pornography; files containing images and data of any type relating to the sexual exploitation of minors, and material related to the possession or production thereof, as defined in 18 U.S.C. §§ 2251 and/or 2252;
- c. Information, correspondence, records, documents, or other materials pertaining to the possession, receipt, or distribution of visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256, or pertaining to the sexual exploitation of minors;
- d. Information, correspondence, records, documents, or other materials pertaining to any scheme or artifice to defraud another individual, as defined in 18 U.S.C. § 1343;
- e. Communications between the user ID and others from January 1, 2022 through May 5, 2025;

- f. Evidence indicating how and when the Facebook account was accessed or used, to determine the geographic and chronological context of account access, use, and events relating to the crime under investigation and to the Facebook account owner;
- g. Evidence indicating the Facebook account owner's state of mind as it relates to the crime under investigation; and
- h. The identity of the person(s) who created or used the user ID, including records that help reveal the whereabouts of such person(s).